Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)
	)
Facilitating Opportunities for Flexible,	)
Efficient, and Reliable Spectrum	) ET Docket No. 03-108
Use Employing Cognitive Radio	)
Technologies	)

EX PARTE STATEMENT

OF

MARCUS SPECTRUM SOLUTIONS

In accordance with the provisions of 47 CFR §1.1206 Marcus Spectrum Solutions (MSS) is filing this *ex parte* statement dealing with the reconsideration of the Report and Order[1] in this proceeding, adopted March 10, 2005. MSS[2] is an independent consulting firm specializing in spectrum technology and policy issues. In this statement MSS is acting in the public interest, not on behalf of a specific client. The Commission is aware of the qualifications[3] of Dr. Michael J. Marcus, Director of MSS.

The main purpose of this filing is to submit into the record Attachment 1, an article from the respected business publication, *Forbes* magazine, entitled "**Does Open-Source Software Make The FCC Irrelevant?**"

The article describes how a loophole in the original software defined radio (SDR) rules adopted in Docket 00-47[4] allowed the legal marketing of radio systems that may have features that are readily exploited by hackers. For example, a very popular Wi-Fi wireless router sold by a reputable company has become known, according to the article, as "for hackers what a Model A Ford was for hotrodders in an earlier era--a highly

---

[1] Published at 70 FR 23039, May 4, 2005.

[2] *See* http://www.marcus-spectrum.com

[3] *See* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-243463A1.pdf

[4] *First Report and Order* in ET Docket No. 00-47, 16 FCC Rcd 17373,17377 (2001).

adaptable platform for experimentation." As an example of the changes that can be made with hacked software, one web page says the power can be increased from 28 mW to 251 mW[5] – a near 10 fold increase! A Google search on this model name and the word "hack" recently yielded almost 64,000 hits – a sign of much activity in this area. The first page of the results is included as Attachment 2.

MSS has no doubt that the designers and marketers of this model had only the most benign intentions. They included into their design the software download/update procedures that had been common industry practice for years in 56 kb/s telephone modems – a product line they also made. These software download upload procedures produce real benefits for consumers because they allow a product to be updated to meet evolving standards or to correct software problems in their initial implementation. But such download/update procedures can be "hacked" if they are not safeguarded with strong technical features like authentication to ensure only authorized downloads are permitted.[6] The original SDR rules were *optional* for such devices and *imposed no mandatory regulation of software downloads*.

Why did the Commission do this? The original proceeding was in response to prospective SDR vendors who wanted a clear policy statement that the FCC encouraged and permitted SDRs. Such statements are important in the real world for the capital formation that is key to such cutting edge technology. Without investment and capital formation, radio technology does *not* move from pages of technical journals into the marketplace. Implicit prohibitions or ambiguities in FCC technical regulations raise the investment risk in such technology and thus inhibits technical innovation. Thus the Commission acted properly in making a clear statement that SDR technology was allowed and was welcome.

But many technologies, including SDR, have a dark side also. Because Docket 00-47 focused almost exclusively on the requests of the SDR proponents, the Commission ignored the risk that legitimate manufacturers might unintentionally produce products that could be subverted to antisocial ends or that low tier questionable manufacturers, who did not participate in the proceeding, might take advantage of the same rules. The Commission did *not* balance risks versus benefits and missed the proverbially "ounce of

---

[5] See http://www.theinquirer.net/?article=20200 While this power increase *per se* is within the 47 CFR §15.247 limit for this type of device, such a power increase after the unit leaves the manufacturer raises nagging questions of whether the out-of-band emissions are still within limits and whether the RF safety limits are still met -- questions the FCC's Equipment Authorization Program would *normally* address.

[6] Preventing the "hacking" of consumer electronics is difficult. The recurring "hacking" of CATV set top boxes and DBS receivers in order to receiver video programming without payment shows that even in the cases where hardware providers have a direct financial incentive to prevent "hacking" they have had only partial success. SDR manufacturers have less financial incentive than the multichannel video distributors to prevent "hacking" and thus need regulation to align their incentives closer to the overall public interest.

prevention" opportunity which would have had little or no impact on what the proponents were seeking. Fortunately, this loophole recently was patch up in the R&O in this proceeding with the new §2.1(c) definition of SDR and new §2.944(a)[7].

However, the R&O in this proceeding left unaffected another loophole that raises very similar concerns. This deals with high speed, high power digital-to-analog converters (DACs) with interfaces for common personal computers. **Such devices, if marketed to the general public, would allow any PC to become an SDR transmitter using frequencies selected by software not subject to FCC regulation.**

While Wi-Fi systems like the wireless router described in the article have limited frequency agility around their intended bands, a DAC is inherently capable of intentional emissions on *any* frequency up to 50% of its sample rate and, unless carefully filtered, could have unintentional emissions much higher.

While DACs now are subject to Subpart B of Part 15 of the Commission's Rules, these rules would have no significant impact on the marketing of high speed, high power DACs other than preventing unintentional emissions when the device is *not* connected to an antenna.

As the Forbes article explains, the FCC would most likely be powerless to control the sale of software that converts such DACs to antisocial uses. Whereas the loophole in the SDR R&O was due to an oversight, corrected in this proceeding, the problem in the DAC case would be statutory and possibly constitutional barriers to regulating software – significantly more difficult to solve.

A previous MSS filing in this proceeding[8] documented hacker interest in using video

---

[7] "§ 2.1(c) *Software defined radio.* A radio that includes a transmitter in which the operating parameters of frequency range, modulation type or maximum output power (either radiated or conducted), or the circumstances under which the transmitter operates in accordance with Commission rules, can be altered by making a change in software without making any changes to hardware components that affect the radio frequency emissions.
§ 2.944 Software defined radios. (a) Manufacturers must take steps to ensure that only software that has been approved with a software defined radio can be loaded into the radio. The software must not allow the user to operate the transmitter with operating frequencies, output power, modulation types or other radio frequency parameters outside those that were approved. Manufacturers may use means including, but not limited to the use of a private network that allows only authenticated users to download software, electronic signatures in software or coding in hardware that is decoded by software to verify that new software can be legally loaded into a device to meet these requirements and must describe the methods in their application for equipment authorization."

[8] *See* Marcus Spectrum Solutions *Reply to Opposition to Petition for Reconsideration*, August 19, 2005,
http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6518148263 ,
http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6518148264 ,
http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6518148265

cards – a low power specialized type of DAC – as radio transmitters. So in view of shown hacker interest in both videocards and wireless routers it is not hard to predict similar interest in high speed, high power DACs if they reach the consumer market.

Fortunately, high speed, high power DACs are *not* on the market yet. Whereas regulating software raises statutory and constitutional issues, as well as practical problems, regulating DAC hardware is clearly authorized under the provisions of §302(a)[9] of the Communications Act of 1934, as amended.

Present high speed DACs have less than 1 Watt power and are very expensive. But the lessons of the past 20 years about advances in computer technology tell us that change can come very fast -- particularly compared to the time required for FCC rulemakings.

This problem described above could be avoided by the minimal regulation of DACs, such as was proposed in the MSS Reconsideration Petition[10]. MSS is empathetic to the concerns raised by Information Technology Industry Association, the PC trade association, in its Opposition[11]. Regulation is never popular. But in recognizing and allowing new technology such as SDR and cognitive radio the Commission should also seek **minimally intrusive ways** to prevent the type of possible spectrum chaos as described in the *Forbes* article. The narrowly crafted MSS proposal[12] for DAC

---

[9] 47 USC §302a(a): "The Commission may, consistent with the public interest, convenience, and necessity, make reasonable regulations (1) governing the interference potential of devices which in their operation are capable of emitting radio frequency energy by radiation, conduction, or other means in sufficient degree to cause harmful interference to radio communications; …"

[10] http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6517623374

[11] http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6518114780

[12] The specific proposal was,
"MSS urges the Commission to issue a Further Notice of Proposed Rulemaking on the issue of D/A converters as opposed to lack of action in the R&O. The FNPRM should propose a very narrowly drawn rule that would only cover D/A converters that met all these qualifications:

1) have sample speeds in excess of 1 million samples/sec *and*
2) have output power greater than 1 Watt *and*
3) have an interface for receiving the digital input to the D/A converter which is interoperable with widely available Class B personal computer systems (*e.g.* USB and Firewire) *and*
4) have an analog output for the converted signal which is compatible in both connector type and approximate impedance with widely available antennas (*e.g.* BNC)

D/A converters meeting all these characteristics would then be classified as Class A digital devices automatically and their marketing to the general public as standalone endproducts would be prohibited. However, they could be included as internal components of broader systems that did not meet the 4 point test. And they could be sold through specialized channels such as the market for electronic test equipment." MSS *Reconsideration Petition* at p. 8

regulation is one possible way to strike such a balance in this area.

Perhaps ITIA might want to make a reasonable counterproposal rather than stonewalling *any* new regulation for products that don't even exist yet? MSS respectfully requests the Commission consider the new issues raised in the attached article.

[I expect to be visiting FCC the week of November 7th in conjunction with *ex parte* presentations on another proceeding. I would be glad to discuss these points further at that time, if asked, and then make an appropriate additional filing.]

October 27, 2005

/s/

Michael J. Marcus, Sc.D., FIEEE
Director, Marcus Spectrum Solutions
October 24, 2005

55, rue Molitor
F-75106 Paris, France
www.marcus-spectrum.com

Copies have been sent by e-mail to the following FCC staffers:

Fred Campbell
John Justi
Barry Ohlson
John Branscome
Bruce Franca
Julius Knapp
Alan Scrime
Rashmi Doshi
Karen Rackley
Hugh vanTuyl
William Lane
Keith Larson
Joseph Casey
George Dillon
James Higgins

Attachment 1 –

Does Open-Source Software Make The FCC Irrelevant?

Daniel Fisher, 10.18.05, 10:00 AM ET

http://www.forbes.com/businesstech/2005/10/18/open-source-software-FCC_cz_df_1018opensource.html?partner=rss

NEW YORK – Columbia Law School Professor Eben Moglen wants to destroy the Federal Communications Commission. Not as some kind of terrorist act, but because technology is rapidly making it irrelevant.

The agency might have made sense in the 1920s, Moglen says, when it was formed to assign specific frequencies to broadcasters so they wouldn't try to drown each other out by cranking up the transmitter power. But a new generation of intelligent radios, combined with equally clever computer networks, is making it possible for anybody to use the airwaves without interfering with anybody else.

That raises the question of why Rupert Murdoch, say, needs exclusive access to a slice of the radio spectrum for his Fox television network when he could just as easily put his content out over the Internet for customers to pick up using low-powered wi-fi receivers hooked into the Web.

"My goal is to do all of the work it takes to be explaining to the Supreme Court in 2025 why broadcasting is unconstitutional," says Moglen, who speaks in perfect, rolling sentences. "We have a long march to do, we have a lot of education to do, society has to catch up with our vision of the future, but we are going someplace and the only question is timing and skill in driving."

Moglen's comments would be easy to dismiss, except for the woe he's already caused the software industry. For nearly a decade, Moglen has been the chief legal officer at the Free Software Foundation, in charge of defending the General Public License, a subversive bit of lawyering that turns property law on its head by prohibiting the users of open-source software from charging money for it.

A polymath who wrote code for IBM in the 1970s while he was earning a law degree and a Ph.D in history at Yale, Moglen enjoys using the tools of capitalism against itself. He's wrung significant concessions out of software companies without filing a suit, including forcing Cisco Systems to "open up" the code in Linksys routers soon after it bought the company for $500 million in 2003.

"I was always able to begin that phone call with the magic words "I don't want money,'" Moglen says, chuckling. "I only want you to play by the rules."

Because open-source software is so easy to modify and use, businesses have embraced it, and millions of people have installed the Linux operating system on their computers. Now entire nations, including Brazil and Venezuela, have committed themselves to using open-source code. The majority of commercial Web servers run on open-source Apache software.

The spread of open source is a threat to established broadcasters, not to mention cellular telephone companies and other holders of FCC licenses. By using open-source software and low-powered "mesh networks" that can sniff out open frequencies and transmit over them, Moglen says, "we can produce bandwidth in a very collaborative way," including transmitting video and telephone conversations that would normally ride on commercial networks. **The Linksys WRT54G wireless router is for hackers what a Model A Ford was for hotrodders in an earlier era--a highly adaptable platform for experimentation.**

"We remove the proprietary software and install open source," says Sascha Meinrath, co-founder of a group that is providing Urbana, Ill. with free wireless Internet access. By "flashing" communications chips with new instructions downloaded off the Internet, Meinrath says, hackers can add sophisticated features to wireless routers such as the ability to adjust frequency and signal power.

That allows more users to occupy the same crowded slice of radio spectrum. But the same code can just as easily allow users to transmit on frequencies the FCC has licensed to somebody else.

Should the FCC try to crack down, the hackers have a powerful weapon: The First Amendment. An offshoot of the Free Software Foundation called GNU Radio is developing a new generation of radios and TV receivers that use software for just about everything except the antenna and the power source. The FCC can prohibit manufacturers from selling radios that transmit on illegal frequencies, but it would have trouble shutting down a Web site distributing software that does the same thing.

"You cannot regulate code without going through the First Amendment-type balancing tests we have for any other type of speech," says Cindy Cohn, a lawyer at the Electronic Freedom Foundation in San Francisco. "Code is speech."

Broadcasters fear that an unregulated community of hackers could throw the airwaves into chaos.

"There's a reason there is the FCC--to protect the integrity of the broadcast band," says Dan Wharton, spokesman for the National Association of Broadcasters in Washington, D.C. "We're very concerned about the potential for interference." *(Emphasis added)*

Techies assume they can solve such problems with better software. But regulators have to anticipate that people will try to drown each other out with transmitter power, says Gerald Faulhaber, a former chief economist for the FCC who now teaches at the University of Pennsylvania's Wharton School of Business.

“Engineers want people to be good,” Faulhaber says. “Economists assume everybody is bad. And guess what? We're right.”

But Moglen believes his First Amendment arguments will trump such objections. Not only will the government have difficulty prosecuting millions of consumers using open-source radios to broadcast on unauthorized frequencies, he says, but the very act of using the airwaves in that manner will make it harder to defend the monopolies granted broadcasters like Fox.

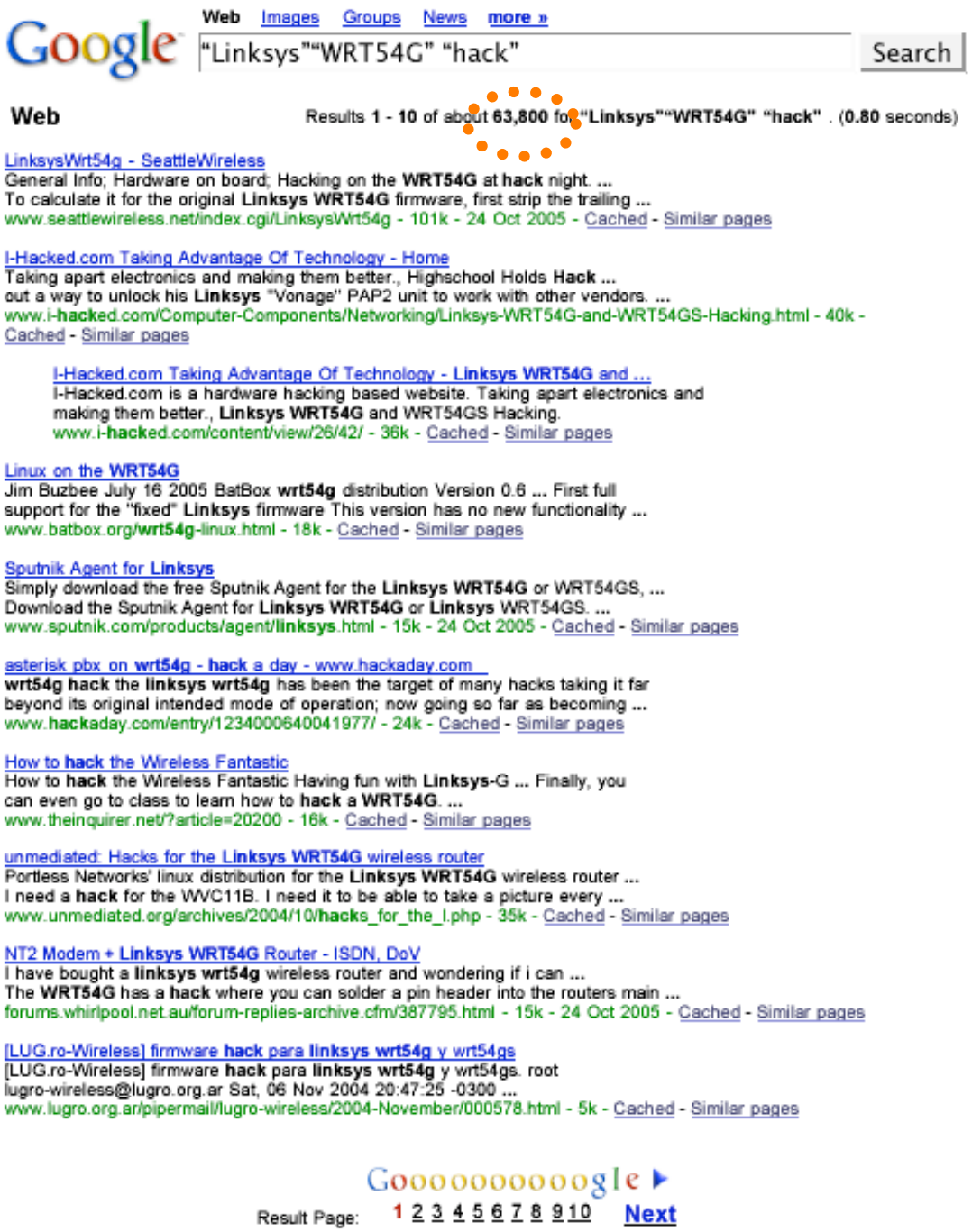
“We've known forever that licensing newspapers is against the rules, so why should radio spectrum be any different?” he says.

Moglen’s 20-year march to the Supreme Court may already have begun. **The FCC is in the midst of a proceeding to determine how it will regulate so-called “cognitive radios,” which use software to switch power and frequency. Hackers are hard at work refining such devices in the cooperative world of open source, where software writers post their code on the Internet and others modify it or offer suggestions.** *(Emphasis added)*

And companies like Cisco, IBM and Computer Associates are hastening the process along, partly as a way of competing with Microsoft They've even put $4.3 million into a public interest law firm Moglen installed in New York offices to enforce the GPL.

“It's really a mistake for capitalists to assume that in these areas--software, information, data--that the best way of guaranteeing the production of this valuable material is the old way [of selling over government-authorized networks]," Moglen says. “There is something different going on here.”

Attachment 2 – Google search results



Google Web Images Groups News more »

"Linksys""WRT54G" "hack" Search

Web Results 1 - 10 of about 63,800 for "Linksys""WRT54G" "hack" . (0.80 seconds)

LinksysWrt54g - SeattleWireless
General Info; Hardware on board; Hacking on the **WRT54G** at **hack** night. ...
To calculate it for the original **Linksys WRT54G** firmware, first strip the trailing ...
www.seattlewireless.net/index.cgi/LinksysWrt54g - 101k - 24 Oct 2005 - Cached - Similar pages

I-Hacked.com Taking Advantage Of Technology - Home
Taking apart electronics and making them better., Highschool Holds **Hack** ...
out a way to unlock his **Linksys** "Vonage" PAP2 unit to work with other vendors. ...
www.i-**hack**ed.com/Computer-Components/Networking/Linksys-WRT54G-and-WRT54GS-Hacking.html - 40k - Cached - Similar pages

I-Hacked.com Taking Advantage Of Technology - **Linksys WRT54G** and ...
I-Hacked.com is a hardware hacking based website. Taking apart electronics and making them better., **Linksys WRT54G** and WRT54GS Hacking.
www.i-**hack**ed.com/content/view/26/42/ - 36k - Cached - Similar pages

Linux on the **WRT54G**
Jim Buzbee July 16 2005 BatBox **wrt54g** distribution Version 0.6 ... First full support for the "fixed" **Linksys** firmware This version has no new functionality ...
www.batbox.org/**wrt54g**-linux.html - 18k - Cached - Similar pages

Sputnik Agent for **Linksys**
Simply download the free Sputnik Agent for the **Linksys WRT54G** or WRT54GS, ...
Download the Sputnik Agent for **Linksys WRT54G** or **Linksys** WRT54GS. ...
www.sputnik.com/products/agent/**linksys**.html - 15k - 24 Oct 2005 - Cached - Similar pages

asterisk pbx on **wrt54g** - **hack** a day - www.hackaday.com
wrt54g hack the **linksys wrt54g** has been the target of many hacks taking it far beyond its original intended mode of operation; now going so far as becoming ...
www.**hack**aday.com/entry/1234000640041977/ - 24k - Cached - Similar pages

How to **hack** the Wireless Fantastic
How to **hack** the Wireless Fantastic Having fun with **Linksys**-G ... Finally, you can even go to class to learn how to **hack** a **WRT54G**. ...
www.theinquirer.net/?article=20200 - 16k - Cached - Similar pages

unmediated: Hacks for the **Linksys WRT54G** wireless router
Portless Networks' linux distribution for the **Linksys WRT54G** wireless router ...
I need a **hack** for the WVC11B. I need it to be able to take a picture every ...
www.unmediated.org/archives/2004/10/**hacks**_for_the_l.php - 35k - Cached - Similar pages

NT2 Modem + **Linksys WRT54G** Router - ISDN, DoV
I have bought a **linksys wrt54g** wireless router and wondering if i can ...
The **WRT54G** has a **hack** where you can solder a pin header into the routers main ...
forums.whirlpool.net.au/forum-replies-archive.cfm/387795.html - 15k - 24 Oct 2005 - Cached - Similar pages

[LUG.ro-Wireless] firmware **hack** para **linksys wrt54g** y wrt54gs
[LUG.ro-Wireless] firmware **hack** para **linksys wrt54g** y wrt54gs. root lugro-wireless@lugro.org.ar Sat, 06 Nov 2004 20:47:25 -0300 ...
www.lugro.org.ar/pipermail/lugro-wireless/2004-November/000578.html - 5k - Cached - Similar pages

Gooooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**